ID: 882716
Sample Name:
D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe
Cookbook: default.jbs
Time: 17:25:18
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

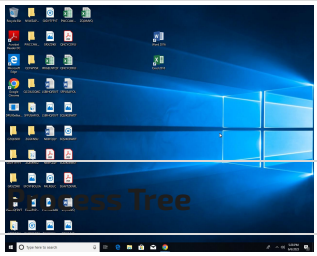
Windows Analysis Report

D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe

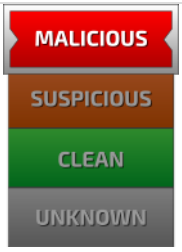
Overview

General Information

Sample Name:	D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe
Original Sample Name:	Dtails_des_tran..
Analysis ID:	882716
MD5:	c2410682e7efc..
SHA1:	ebca329924db…
SHA256:	8977050efc90a..
Tags:	exe
Infos:	



Detection



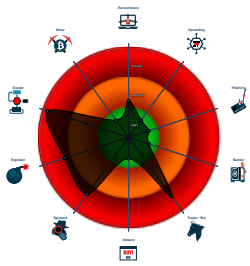
AgentTesla

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dom…
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- .NET source code references suspic…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe (PID: 5644 cmdline: C:\Users\user\Desktop\D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe MD5: C2410682E7EFC9A89F4C88AC2BD51FD1)
  - RegAsm.exe (PID: 6512 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe MD5: 2B5D765B33C67EBA41E9F47954227BC3)
  - csc.exe (PID: 6484 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe MD5: B46100977911A0C9FB1C3E5F16A5017D)
  - AddInProcess32.exe (PID: 1288 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
- Myapp.exe (PID: 6864 cmdline: "C:\Users\user\AppData\Roaming\Myapp\Myapp.exe" MD5: F2A47587431C466535F3C3D3427724BE)
  - conhost.exe (PID: 6872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Myapp.exe (PID: 7012 cmdline: "C:\Users\user\AppData\Roaming\Myapp\Myapp.exe" MD5: F2A47587431C466535F3C3D3427724BE)
  - conhost.exe (PID: 7020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.securework s.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.co m/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http:// https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.glassy.com.tr",
  "Username": "info@glassy.com.tr",
  "Password": "Sc2017*"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.605388772.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.361896473.0000026754CAD000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000003.00000002.606232298.0000000002D01000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.606232298.0000000002D01000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.363891245.0000026764C61000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe.26764d1d9b8.3.unpack	MSIL_SUSP_OBFUSC_XorStringsNet	Detects XorStringsNET string encryption, and other obfuscators derived from it	dr4k0nia	• 0x18103:$pattern: 06 1E 58 07 8E 69 FE 17 • 0x26f22:$a2: _CorExeMain • 0x22cc0:$a3: mscorlib • 0x240ed:$a4: .cctor • 0x22a3d:$a6: <Module>
0.2.D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe.26764d1d9b8.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe.26764cbf970.2.unpack	MSIL_SUSP_OBFUSC_XorStringsNet	Detects XorStringsNET string encryption, and other obfuscators derived from it	dr4k0nia	• 0x18103:$pattern: 06 1E 58 07 8E 69 FE 17 • 0x26f22:$a2: _CorExeMain • 0x22cc0:$a3: mscorlib • 0x240ed:$a4: .cctor • 0x22a3d:$a6: <Module>
0.2.D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe.26764cbf970.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.AddInProcess32.exe.400000.0.unpack	MSIL_SUSP_OBFUSC_XorStringsNet	Detects XorStringsNET string encryption, and other obfuscators derived from it	dr4k0nia	• 0x19f03:$pattern: 06 1E 58 07 8E 69 FE 17 • 0x28d22:$a2: _CorExeMain • 0x24ac0:$a3: mscorlib • 0x25eed:$a4: .cctor • 0x2483d:$a6: <Module>

Click to see the 8 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for sample
- Sample uses string decryption to hide its real strings

Exploits

- Yara detected UAC Bypass using CMSTP

System Summary

- Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect sandboxes / dynamic malware analysis system (file name check)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

- Writes to foreign memory regions
- .NET source code references suspicious native API functions
- Injects a PE file into a foreign processes

Stealing of Sensitive Information

- Yara detected AgentTesla
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

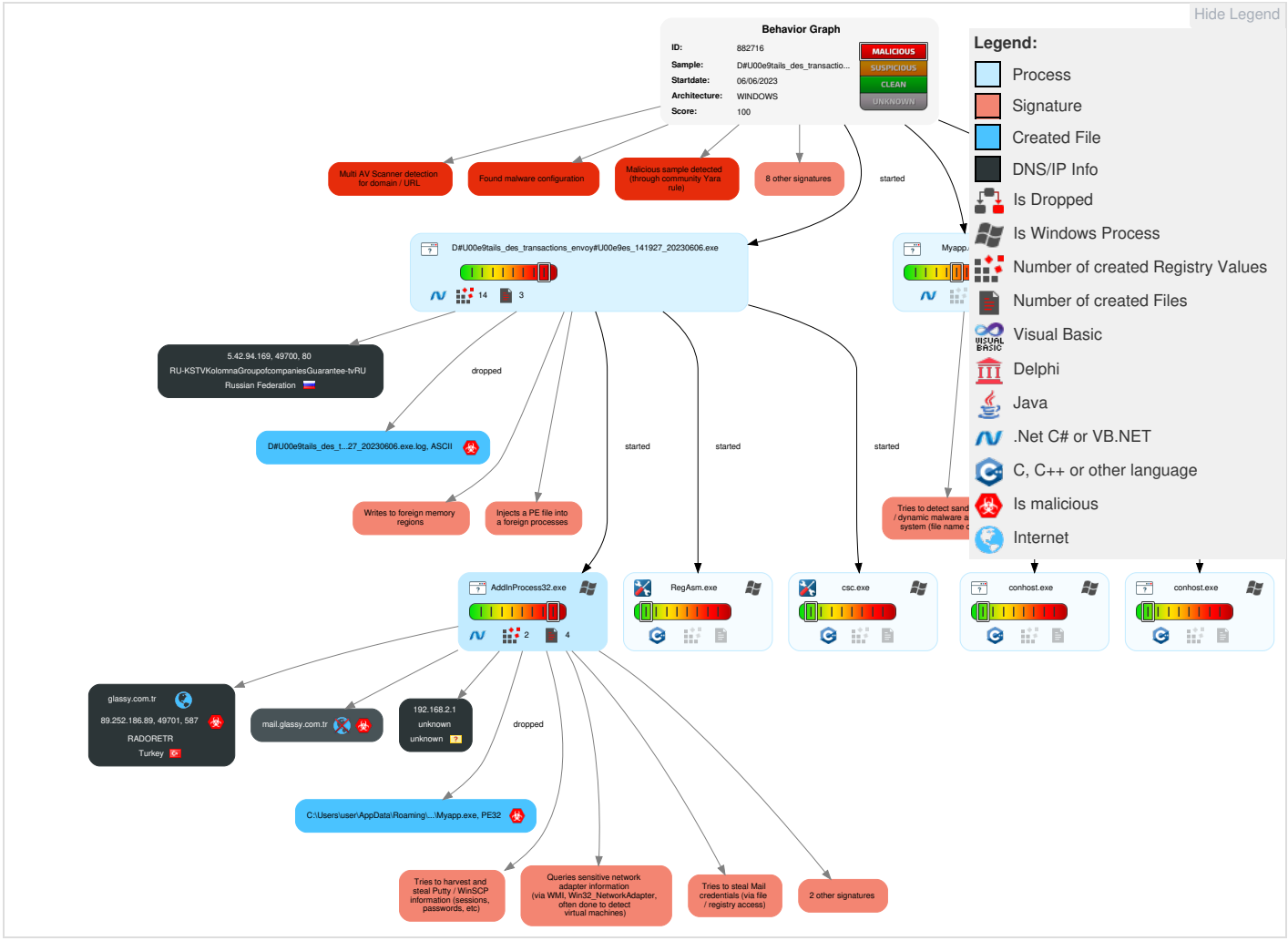
- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	2 1 1 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	2 4 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 3 1 Virtualization/Sandbox Evasion	LSA Secrets	2 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 1 Process Injection	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	1 System Owner/User Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

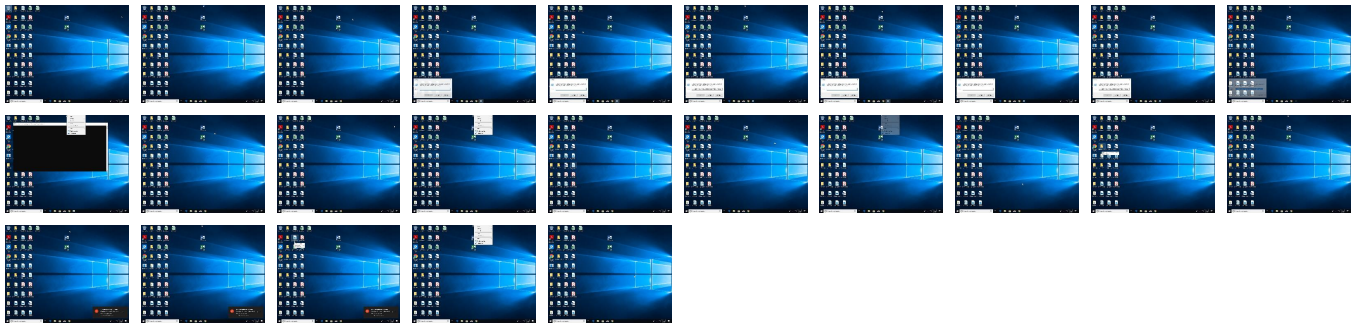
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe	11%	Virustotal		Browse
D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Myapp\Myapp.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
glassy.com.tr	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/ocsp0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/DPCyPoliticas0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://5.42.94.169	0%	Avira URL Cloud	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://5.42.94.169	8%	Virustotal		Browse
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	URL Reputation	safe	
http://glassy.com.tr	0%	Virustotal		Browse
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://ocsp.ncdc.gov.sa0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://glassy.com.tr	0%	Avira URL Cloud	safe	
http://www.uce.gub.uy/acrn/acrn.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://www.agesic.gub.uy/acrn/acrn.crl0)	0%	URL Reputation	safe	
http://www.rcsc.lt/repository0	0%	URL Reputation	safe	
http://www2.postsignum.cz/crl/psrootqca2.crl01	0%	URL Reputation	safe	
http://r3.i.lencr.org/0?	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0?	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
glassy.com.tr	89.252.186.89	true	true	• 0%, Virustotal, Browse	unknown
mail.glassy.com.tr	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	AddInProcess32.exe, 00000003.00000003.38 1062942.0000000005FAD000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380380699.0000000005FA400 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	AddInProcess32.exe, 00000003.00000003.38 0956339.0000000006BF4000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.e-me.lv/repository0	AddInProcess32.exe, 00000003.00000003.38 0230644.0000000006C7B000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	AddInProcess32.exe, 00000003.00000003.38 0956339.0000000006BF4000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380553103.0000000005F5300 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	AddInProcess32.exe, 00000003.00000003.38 0524565.0000000005F5D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	AddInProcess32.exe, 00000003.00000003.38 0956339.0000000006BF4000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380446191.0000000005F6800 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	AddInProcess32.exe, 00000003.00000003.38 0683980.0000000005F44000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	AddInProcess32.exe, 00000003.00000003.38 0317982.0000000006C65000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	AddInProcess32.exe, 00000003.00000003.38 0956339.0000000006BF4000.00000004.000000 20.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.chambersign.org1	AddInProcess32.exe, 00000003.00000003.38 0608355.0000000006C63000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380524565.0000000005F5D00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	AddInProcess32.exe, 00000003.00000003.38 0230644.0000000006C6D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://repository.swisssign.com/0	AddInProcess32.exe, 00000003.00000003.38 0956339.0000000006BF4000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380446191.0000000005F6800 0.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.38068398 0.0000000005F44000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	AddInProcess32.exe, 00000003.00000003.38 0956339.0000000006BF4000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380446191.0000000005F6800 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	AddInProcess32.exe, 00000003.00000003.38 0524565.0000000005F5D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	AddInProcess32.exe, 00000003.00000003.38 0230644.0000000006C6D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	AddInProcess32.exe, 00000003.00000003.38 0683980.0000000005F44000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	AddInProcess32.exe, 00000003.00000003.38 0317982.0000000006C65000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	AddInProcess32.exe, 00000003.00000003.38 1009579.0000000005F3A000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380718660.0000000005F3500 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	AddInProcess32.exe, 00000003.00000003.38 0230644.0000000006C6D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	AddInProcess32.exe, 00000003.00000003.38 0956339.0000000006BF4000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380446191.0000000005F6800 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/root2.crl0	AddInProcess32.exe, 00000003.00000003.38 0380699.0000000005FA4000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	AddInProcess32.exe, 00000003.00000003.38 0524565.0000000005F5D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	AddInProcess32.exe, 00000003.00000003.38 0317982.0000000006C65000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sk.ee/cps/0	AddInProcess32.exe, 00000003.00000003.38 0446191.0000000005F68000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.globaltrust.info0=	AddInProcess32.exe, 00000003.00000003.38 0608355.0000000006C63000.00000004.000000 20.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	AddInProcess32.exe, 00000003.00000003.38 0446191.0000000005F68000.00000004.000000 20.00020000.00000000.sdmp	false		high
http:// www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	AddInProcess32.exe, 00000003.00000003.38 0718660.0000000005F35000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380875195.0000000005F4300 0.00000004.00000020.00020000.00000000.sdmp	false		high

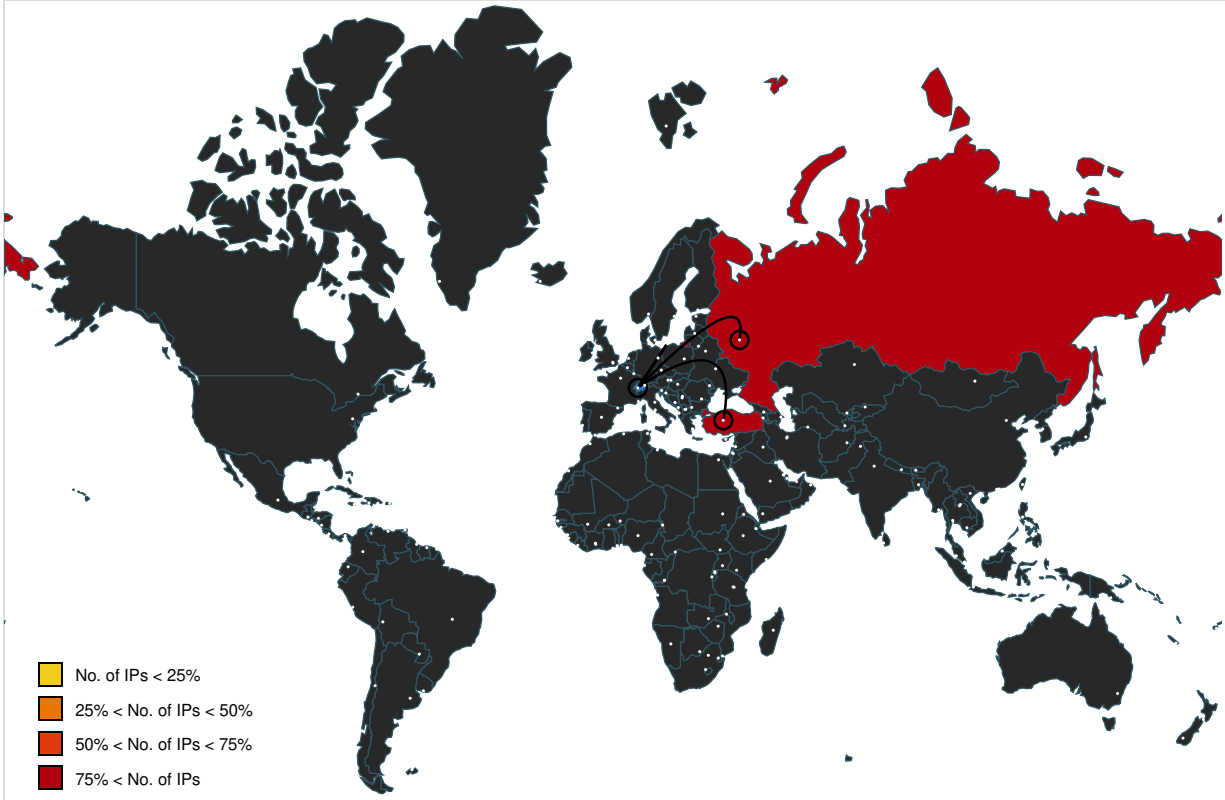
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe, 00000000.00000002.361896473.0000026754C41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pki.registradores.org/normativa/index.htm0	AddInProcess32.exe, 00000003.00000003.380230644.0000000006C6D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	AddInProcess32.exe, 00000003.00000002.610257702.0000000005F83000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000002.609957229.0000000005EB8000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000002.606232298.0000000002D5A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://policy.camerfirma.com0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380524565.0000000005F5D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ssc.lt/cps03	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380230644.0000000006C6D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	AddInProcess32.exe, 00000003.00000003.380683980.0000000005F44000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	AddInProcess32.exe, 00000003.00000003.380757354.0000000006BFE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	AddInProcess32.exe, 00000003.00000003.380718660.0000000005F35000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380524565.0000000005F5D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://5.42.94.169	D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe, 00000000.00000002.361896473.0000026754C41000.00000004.00000800.00020000.00000000.sdmp	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	AddInProcess32.exe, 00000003.00000003.380524565.0000000005F5D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	AddInProcess32.exe, 00000003.00000002.605694979.0000000001005000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000002.609957229.0000000005EB8000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.425558872.0000000000FDC000.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000002.606232298.0000000002D5A000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000002.605694979.0000000000FDF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://glassy.com.tr	AddInProcess32.exe, 00000003.00000002.606232298.0000000002D5A000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	AddInProcess32.exe, 00000003.00000003.380553103.0000000005F53000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	AddInProcess32.exe, 00000003.00000003.380742001.0000000005F2E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	AddInProcess32.exe, 00000003.00000003.380553103.0000000005F53000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	AddInProcess32.exe, 00000003.00000003.381033686.0000000006BEB000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wwww.certigna.fr/autorites/0m	AddInProcess32.exe, 00000003.00000003.380317982.0000000006C65000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.dnie.es/dpc0	AddInProcess32.exe, 00000003.00000003.380718660.0000000005F35000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.mtin.es/mtin/DPCyPoliticas0	AddInProcess32.exe, 00000003.00000003.380524565.0000000005F5D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	AddInProcess32.exe, 00000003.00000003.380757354.0000000006BFE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	AddInProcess32.exe, 00000003.00000003.380608355.0000000006C63000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://crl.anf.es/AC/ANFServerCA.crl0	AddInProcess32.exe, 00000003.00000003.380757354.0000000006BFE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.certeurope.fr/reference/pc-root2.pdf0	AddInProcess32.exe, 00000003.00000003.380380699.0000000005FA4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ac.economia.gob.mx/last.crl0G	AddInProcess32.exe, 00000003.00000003.380608355.0000000006C63000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.catcert.net/verarrel	AddInProcess32.exe, 00000003.00000003.380230644.0000000006C6D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca0f	AddInProcess32.exe, 00000003.00000003.380317982.0000000006C65000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	AddInProcess32.exe, 00000003.00000003.380683980.0000000005F44000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	AddInProcess32.exe, 00000003.00000003.380230644.0000000006C6D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	AddInProcess32.exe, 00000003.00000003.380608355.0000000006C63000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	AddInProcess32.exe, 00000003.00000003.380718660.0000000005F35000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.quovadis.bm0	AddInProcess32.exe, 00000003.00000003.380956339.0000000006BF4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	AddInProcess32.exe, 00000003.00000003.380553103.0000000005F53000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.accv.es00	AddInProcess32.exe, 00000003.00000003.38 0683980.0000000005F44000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	AddInProcess32.exe, 00000003.00000003.38 0446191.0000000005F68000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.netlock.net/docs	AddInProcess32.exe, 00000003.00000003.38 0718660.0000000005F35000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_ 1.pdf0	AddInProcess32.exe, 00000003.00000003.38 0524565.0000000005F5D000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://www.e-trust.be/CPS/QNcerts	AddInProcess32.exe, 00000003.00000003.38 0718660.0000000005F35000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380524565.0000000005F5D00 0.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.38023064 4.0000000006C7B000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.ncdc.gov.sa0	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	AddInProcess32.exe, 00000003.00000003.38 1033686.0000000006BEB000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://trustcenter- crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA. crl0	AddInProcess32.exe, 00000003.00000003.38 0683980.0000000005F44000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	AddInProcess32.exe, 00000003.00000003.38 0446191.0000000005F68000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380683980.0000000005F4400 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	AddInProcess32.exe, 00000003.00000003.38 1009579.0000000005F3A000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380718660.0000000005F3500 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://repository.luxtrust.lu0	AddInProcess32.exe, 00000003.00000003.38 0230644.0000000006C6D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	AddInProcess32.exe, 00000003.00000003.38 0524565.0000000005F5D000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org0	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.i.lencr.org/0?	AddInProcess32.exe, 00000003.00000002.60 5694979.0000000001005000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000002.609957229.0000000005EB800 0.00000004.00000020.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.42555887 2.0000000000FDC000.00000004.00000020.000 20000.00000000.sdmp, AddInProcess32.exe, 00000003.00000002.606232298.0000000002D 5A000.00000004.00000800.00020000.0000000 0.sdmp, AddInProcess32.exe, 00000003.000 00002.605694979.0000000000FDF000.0000000 4.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ocsp.eca.hinet.net/OCSP/ocspG2sha20	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://www.firmaprofesional.com/cps0	AddInProcess32.exe, 00000003.00000003.38 1009579.0000000005F3A000.00000004.000000 20.00020000.00000000.sdmp, AddInProcess32.exe, 00000003.00000003.380718660.0000000005F3500 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/acrn/acrn.crl0	AddInProcess32.exe, 00000003.00000003.38 0553103.0000000005F53000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.securetrust.com/SGCA.crl0	AddInProcess32.exe, 00000003.00000002.60 9957229.0000000005EB0000.00000004.000000 20.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	AddInProcess32.exe, 00000003.00000003.380553103.0000000005F53000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agesic.gub.uy/acrn/acrn.crl0)	AddInProcess32.exe, 00000003.00000003.380553103.0000000005F53000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rcsc.lt/repository0	AddInProcess32.exe, 00000003.00000003.380683980.0000000005F44000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www2.postsignum.cz/crl/psrootqca2.crl01	AddInProcess32.exe, 00000003.00000003.380683980.0000000005F44000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	AddInProcess32.exe, 00000003.00000003.380446191.0000000005F68000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	AddInProcess32.exe, 00000003.00000003.380230644.0000000006C6D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.quovadisglobal.com/cps0	AddInProcess32.exe, 00000003.00000003.380230644.0000000006C6D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl0	AddInProcess32.exe, 00000003.00000003.380683980.0000000005F44000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.42.94.169	unknown	Russian Federation		39493	RU-KSTVKolomnaGroupofcompaniesGuarantee-tvRU	false
89.252.186.89	glassy.com.tr	Turkey		42926	RADORETR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882716
Start date and time:	2023-06-06 17:25:18 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe
Original Sample Name:	Dtails_des_transactions_envoyes_141927_20230606.exe
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winEXE@11/5@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 0.9%) • Quality average: 44.1% • Quality standard deviation: 39.9%
HCA Information:	• Successful, ratio: 60% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 8.238.88.248, 8.238.88.126, 8.248.141.254, 8.238.88.120, 8.248.119.254, 93.184.221.240
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:26:19	API Interceptor	57x Sleep call for process: D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe modified
17:26:30	API Interceptor	37x Sleep call for process: AddInProcess32.exe modified
17:26:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Myapp C:\Users\user\AppData\Roaming\Myapp\Myapp.exe
17:26:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Myapp C:\Users\user\AppData\Roaming\Myapp\Myapp.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 63843 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	63843
Entropy (8bit):	**7.99568798138569**
Encrypted:	**true**
SSDEEP:	1536:MRxM2u+06GOIVUvVmMKAfUfsrPa1jfCu18ZNMe3v:KMH+F3lacMZ2CPACu1GN7v
MD5:	3AC860860707BAAF32469FA7CC7C0192
SHA1:	C33C2ACDABA0E6FA41FD2F00F186804722477639
SHA-256:	D015145D551ECD14916270EFAD773BBC9FD57FAD2228D2C24559F696C961D904
SHA-512:	D62AD2408C969A95550FB87EFDA50F988770BA5E39972041BF85924275BAF156B8BEC309ECC6409E5ACDD37EC175DEA40EFF921AB58933B5B5B5D35A6147567C
Malicious:	false
Preview:	MSCF....c.....,.....I.....V. .authroot.stl....e/5..CK..8U....a..t2.1.P. J.".t..2F2e....&))$7*I.4...e...+SJE...[.T/..{.....c.k....?..Z....bz..qzq.l....,{...i.....39..a.ia....&.3.L2 ...CTf....I7. ....o.2.0a1m.PG.t.....GH.k.6#L.t2.4._.Y!B.h.....NP~..<Z.G..F#..x"f%...x.aF(.J.3...bf7y.j....)...3.....y7UZ..7g~9.....".._.t_"K.S...">..,.....V..}.K.Vv3[...A.9O. .Ea\..+CEv...6CBKt...K..5qa....!..<./X.....r.. ?(.\[. .....y..... ..V.s.`...k@.`.....p...GY..;.`....v..ou.....GH.6.I...P2.(8g.....".....-#...h.U.t..{o./e.wAST.f}0R.(.NM.{...{.=Ch.va'.?W.. .C....T.pw=.W~+.....u.`D.)(*..VdN. .py@...%...YY.>.`.....Y.U.....}...9....\V~=..-...Q....._0.o.nZ....(6.....4.}.`...s.O.K5.W..4.....s,}...6.....'.8&}.{..*...RlZ.?.D4).(.....O.....V..V. pk.:]...,.f`D..e.SO.G.%.:).....eo.bU}.....g..$.gui..h.;-....he(.XoY;..6a..x..`lq...*.:.F!..I.X....!...Lg..53.._....S..G..`...N|..Zx..o.#}Lnd1.V.eE....I.'..`.....KnN....3....{.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.116771890515968
Encrypted:	false
SSDEEP:	6:kKL/SFN+SkQlPlEGYRMY9z+4KlDA3RUeg/U3lWQy:Ta2kPlE99SNxAhUe7oQy
MD5:	63446F335933C67E6F1FAFA0171AFB92
SHA1:	4923BC0A3B8D2FA373FC74A2FC687BB76C344357
SHA-256:	317A3360C5E86399D0DC8B32548BF378FEB61F90DD730A65318522A5BEAE9794
SHA-512:	7AFBE31DB13C79D94BA585512481364DD68C4994F016C54931BF603ACCE08EFBE23698145136149C92F8F8C6873BE10C7378F6BFA12FC804FD867D45B1DBB81
Malicious:	false
Preview:	p..... .....(..... .....w.....(.....c...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".4.6.e.e.f.7.f.b.9.e.7.7.d.9.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe.log

Process:	C:\Users\user\Desktop\D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.378294470225564
Encrypted:	false
SSDEEP:	48:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1hAHKKPFHd+vxpNT:iqnwmI0qerYqGgAoPtzG1eqKPF0ZPT
MD5:	7D3052B85D153A5448F78F234421F934
SHA1:	BA02AA0EA561BB421F48C75C9E55333CFDBF3F58
SHA-256:	DEED3F1305FEDAA4EB6909108258C1A94F174EE1E11D01ED5FD527E941B53B1A
SHA-512:	12D35C9E0F3D18110D5F69F7E0F5276ADF275F70CA85616AB16DD6B776534026237C2F2B3170CE5D1613DD4B2155F967BB0CD370E5220FC2928C92769D1B5E4
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Myapp.exe.log

Process:	C:\Users\user\AppData\Roaming\Myapp\Myapp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.323457581748961
Encrypted:	false
SSDEEP:	12:Q3La/hSoDLI4MWuCIAWDLI4MWuCqDLI4MWuPk21v:MLbAE4KdAmE4K5E4Ks2I
MD5:	9E1D64FA10472A952CB875CE57F99B8F
SHA1:	B00201D8B2B6619400ADE14B761E53F2B76CA8A8
SHA-256:	A1538761E0AD25AFB5372BBC97A5929DD2D714C172CA7F128FBF620809CC2F55
SHA-512:	2E6328BBC14B89B2ACC3C4CA44889816CF58A6F936783C9DDAA0C38F516EE5AECD789800920E4C9FC9988DD3E3CEDCB3096440C1A449989F36EE5448465CDEC
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.AddIn, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Runtime.Remoting, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Roaming\Myapp\Myapp.exe

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6lq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E9D8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....\|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,....r...p.o....-..*.....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&... (-....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.857373989980419
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe
File size:	24576
MD5:	c2410682e7efc9a89f4c88ac2bd51fd1
SHA1:	ebca329924db6f5326250edf8b304b01f26062c2
SHA256:	8977050efc90ae103360367456fd07a930525c1b6cb5ff0f69b90ed21d13ab19
SHA512:	99fc3ad1e88027d24f06d908abe350f95bb14551b0715bd588fef44aa446d48729ee939f51f7e44907e63cd748644331b006a23b18457c3196bc30c9170da5da
SSDEEP:	384:3AMZSCDIjm4ODXJtVfb5xfi6nsbqrmBJu4uViNJPa2mmgY1kwyR2vRM5kwFDh+BW:+m4ODXJtVCeLCfRzRvcFDQa5XhXb
TLSH:	90B25B157BE88722E6FF4F36A4B211805337FAB77122CB1E0AD450A62E537D84A517A3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....0.d....."...0.PS..... ....@..... .....#>....`.....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x647F30F1 [Tue Jun 6 13:13:21 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8000	0x91c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x5c00	0x1798	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5350	0x5400	False	0.5550130208333334	data	6.005205354912129	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x91c	0xa00	False	0.29609375	data	4.331244659117532	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

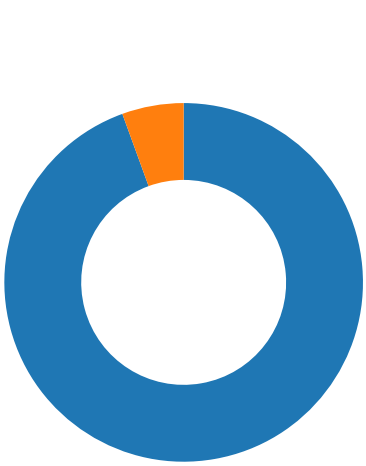
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x80b8	0x33c	data		
RT_VERSION	0x83f4	0x33c	data	English	United States
RT_MANIFEST	0x8730	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:26:18.304310083 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.353907108 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.354109049 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.357033014 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.409200907 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409246922 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409276009 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409305096 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409333944 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409358978 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409382105 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409403086 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409425020 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409446001 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.409475088 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.409475088 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.409475088 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.409475088 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.409535885 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459099054 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459151983 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459178925 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459197998 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459242105 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459269047 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459314108 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459331989 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459345102 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459331989 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459373951 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459407091 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459419012 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459428072 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459451914 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459480047 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459508896 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459511042 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459537029 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459568977 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459584951 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459584951 CEST	49700	80	192.168.2.7	5.42.94.169

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:26:18.459599972 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459621906 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459635973 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459676027 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459705114 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.459732056 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.459769011 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509376049 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509427071 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509458065 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509495020 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509525061 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509552002 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509582996 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509613037 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509644032 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509671926 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509691000 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509691000 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509691000 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509701967 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509691000 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509732008 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509766102 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509793997 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509823084 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509851933 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509879112 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509884119 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509884119 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509884119 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509907961 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509926081 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509936094 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509962082 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.509964943 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.509991884 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510020018 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510020018 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.510051012 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510081053 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510090113 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.510113001 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510140896 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510148048 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.510170937 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510199070 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510199070 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.510230064 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510260105 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510261059 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.510293961 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510314941 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.510344982 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510375023 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510395050 CEST	49700	80	192.168.2.7	5.42.94.169
Jun 6, 2023 17:26:18.510405064 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510437965 CEST	80	49700	5.42.94.169	192.168.2.7
Jun 6, 2023 17:26:18.510463953 CEST	49700	80	192.168.2.7	5.42.94.169

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:26:30.772469044 CEST	50835	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:26:30.807960987 CEST	53	50835	8.8.8.8	192.168.2.7
Jun 6, 2023 17:26:30.817384958 CEST	50505	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:26:30.852183104 CEST	53	50505	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:26:30.772469044 CEST	192.168.2.7	8.8.8.8	0x2c8e	Standard query (0)	mail.glassy.com.tr	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:26:30.817384958 CEST	192.168.2.7	8.8.8.8	0x14dd	Standard query (0)	mail.glassy.com.tr	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 17:26:30.807960987 CEST	8.8.8.8	192.168.2.7	0x2c8e	No error (0)	mail.glassy.com.tr	glassy.com.tr		CNAME (Canonical name)	IN (0x0001)	false
Jun 6, 2023 17:26:30.807960987 CEST	8.8.8.8	192.168.2.7	0x2c8e	No error (0)	glassy.com.tr		89.252.186.89	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:26:30.852183104 CEST	8.8.8.8	192.168.2.7	0x14dd	No error (0)	mail.glassy.com.tr	glassy.com.tr		CNAME (Canonical name)	IN (0x0001)	false
Jun 6, 2023 17:26:30.852183104 CEST	8.8.8.8	192.168.2.7	0x14dd	No error (0)	glassy.com.tr		89.252.186.89	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

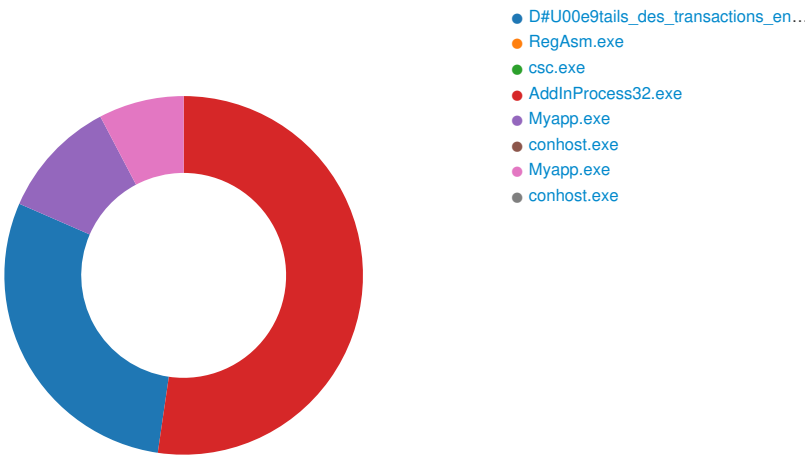
- 5.42.94.169

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 6, 2023 17:26:32.346237898 CEST	587	49701	89.252.186.89	192.168.2.7	220-rd-sacred.guzelhosting.com ESMTP Exim 4.96 #2 Tue, 06 Jun 2023 18:26:31 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 6, 2023 17:26:32.363554001 CEST	49701	587	192.168.2.7	89.252.186.89	EHLO 088753
Jun 6, 2023 17:26:32.412746906 CEST	587	49701	89.252.186.89	192.168.2.7	250-rd-sacred.guzelhosting.com Hello 088753 [102.129.143.77] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPECONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jun 6, 2023 17:26:32.418628931 CEST	49701	587	192.168.2.7	89.252.186.89	STARTTLS
Jun 6, 2023 17:26:32.470731974 CEST	587	49701	89.252.186.89	192.168.2.7	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe PID: 5644, Parent PID: 3320

General

Target ID:	0
Start time:	17:26:16
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe
Imagebase:	0x267530d0000
File size:	24576 bytes
MD5 hash:	C2410682E7EFC9A89F4C88AC2BD51FD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.361896473.0000026754CAD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.363891245.0000026764C61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE220BF1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFE220BF1E9	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE225286ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\D#U00e9tails_des_transactions_envoy#U00e9es_141927_20230606.exe.log	0	1595	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Drawing, Version=4.	success or wait	1	7FFE22528769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE21F8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE21F8B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE220612E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE21F92625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFE220612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFE220612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFE220612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFE220612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFE220612E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFE220612E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE21F8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFE21F8B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFE20EEB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFE20EEB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFE220612E7	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: **6512**, Parent PID: **5644**

General	
Target ID:	1
Start time:	17:26:25
Start date:	06/06/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Imagebase:	0x1ff1f9c0000
File size:	64096 bytes
MD5 hash:	2B5D765B33C67EBA41E9F47954227BC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: **6484**, Parent PID: **5644**

General	
Target ID:	2
Start time:	17:26:26
Start date:	06/06/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Imagebase:	0x7ff738070000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AddInProcess32.exe PID: **1288**, Parent PID: **5644**

General	
Target ID:	3
Start time:	17:26:26
Start date:	06/06/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe
Imagebase:	0x9f0000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.605388772.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.606232298.0000000002D01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.606232298.0000000002D01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E3CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E3CF06	unknown
C:\Users\user\AppData\Roaming\Myapp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C8BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Myapp\Myapp.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71C8DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Myapp\Myapp.exe	0	42080	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1d 5a fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 58 00 00 00 0c 00 00 00 00 00 00 fd 77 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 0d 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELZZ0Xw @ `	success or wait	1	71C8DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	8171	end of file	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	8171	end of file	1	72E1CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	4096	end of file	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\AddInProcess32.exe.config	unknown	8171	end of file	1	72E15705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3d3bfcea-a92d-4141-afde-fa1cf8edbed3	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3d3bfcea-a92d-4141-afde-fa1cf8edbed3	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71C81B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Myapp	unicode	C:\Users\user\AppData\Roaming\Myapp\Myapp.exe	success or wait	1	71C8646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	Myapp	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	71C8DE2E	RegSetValueExW

Analysis Process: Myapp.exe PID: **6864**, Parent PID: **3320**

General

Target ID:	4
Start time:	17:26:41
Start date:	06/06/2023
Path:	C:\Users\user\AppData\Roaming\Myapp\Myapp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Myapp\Myapp.exe"
Imagebase:	0xf00000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Myapp.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7314C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Myapp.exe.log	0	411	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 41 64 64 49 6e 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 52 65 6d 6f 74 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.AddIn, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",02,"System.Runtime.Remoting, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0,	success or wait	1	7314C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile

Analysis Process: conhost.exe PID: **6872**, Parent PID: **6864**

General

Target ID:	5
Start time:	17:26:41
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Myapp.exe PID: **7012**, Parent PID: **3320**

General

Target ID:	6
Start time:	17:26:49
Start date:	06/06/2023
Path:	C:\Users\user\AppData\Roaming\Myapp\Myapp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Myapp\Myapp.exe"
Imagebase:	0x660000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile

Analysis Process: conhost.exe PID: **7020**, Parent PID: **7012**

General

Target ID:	7
Start time:	17:26:50
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly